Security and Privacy of Corporate Income Tax Returns
Discussion Paper – June 2005

Recent events and news concerning disclosures of customer information, presents an appropriate opportunity to discuss the protections that the Internal Revenue Service (IRS) has in place to protect corporate tax return data that is electronically filed and transmitted to IRS.

The Internal Revenue Service is bound by law to protect the privacy of tax return information and meeting that responsibility takes the highest priority at the agency. Information transmitted through IRS e-file is secure because multiple security mechanisms and personnel, operating under strict federal guidelines, carefully protect the information.

Taxpayers cannot file returns directly with the IRS. All electronic returns filed must go through an IRS authorized transmitter. IRS e-file systems employ a variety of security features, which are closely monitored to prevent unauthorized or inappropriate access.

The purpose of this document is to help stakeholders understand some of the numerous processes and procedures the IRS has implemented to protect taxpayer data. This document does not contain specific or exhaustive details about Modernized e-File (MeF) processing within the IRS boundary, because freely disseminating that information would jeopardize the very security we intend to provide.

Security of Return Data During Transmission

In order to transmit electronic return data directly to the IRS, potential Transmitters must first complete a registration and application process, and be verified and approved by IRS officials. Approved Transmitters receive a unique Electronic Filing Identification Number (EFIN), Electronic Transmitter Identification Number (ETIN) and must use it in conjunction with a unique password for authentication.

The MeF design implemented an Internet Filing Application (IFA) to meet the needs of registered transmitters who send large complex returns using a standard web browser. A new release of MeF will add Application to Application (A2A) functionality to support automated submission of return data in a secure manner. The design of the IFA and A2A features Web Services-Interoperability (WS-I) security standards.

IFA and A2A are hosted within the IRS' Modernized System Infrastructure and are accessed through the Registered User Portal (RUP). Transmitters are required to use a unique user name and password in order to log in to the RUP. Once the transmitter successfully logs into the RUP, the SSL Handshake Protocol allows the RUP and transmitter to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the first byte of return data is transmitted. This connection is private. The transmitter and the RUP negotiate a secret encryption key (Transmitter's Browser for the IFA channel and the Transmitter's Web Service Client for the A2A channel) for encrypted communication between the transmitter and the MeF system. This secret key is shared only between the transmitter and the RUP and is not known to any individual. The transmission is part of a secure communications protocol

HTTPS/SSL. The strength of the encryption key used determines the degree of difficulty for anyone to decode the key and thereby decode the return data. IRS uses SSL 3.0 128-bit encryption for access to the RUP. The key created for each transmission is almost impossible to break since using 128-bit creates as many combinations as the number of water molecules in 2.7 million Olympic size swimming pools. The secure SSL tunnel also protects the return data from being intercepted while in transit.

New capabilities require reassessment of deployed technologies therefore additional security measures are under discussion. Additional security mechanisms are also employed to monitor and verify the data source, transmission, and accuracy.

IRS Security

Over the last few years, IRS has implemented a new IRS Modernized System Infrastructure. The Modernized System Infrastructure protects taxpayer information in accordance with the Privacy Act of 1974 (5 USC 552a) through security programs that defend against intrusion, eavesdropping, malicious code and unauthorized access. IRS established the Mission Assurance and Security Services (MA&SS) organization and specifically Modernization and System Security Engineering (M&SSE) and Privacy functions to ensure all systems used to receive, process and store tax return data are secure. ANY AND ALL access to tax return data is protected, fully controlled, monitored, verified, and logged for analysis of abusive or malicious purposes. The design and development of all IRS systems follow a life-cycle process which includes rigorous review of the Functional, Logical, Physical and Security designs.

Before IRS systems are operationally deployed, OMB Circular A-130, and the Federal Information Security Management Act (FISMA) (Title III of the E-Government Act (P.L.107-347)) require that major applications such as MeF undergo a Certification and Accreditation (C&A) Process that is customized to the needs of each agency.

- Certification is a formal review and test of the security safeguards implemented to determine whether the system provides adequate security that is commensurate with the risk of operating the system on the IRS information technology infrastructure.

- Accreditation is the formal authorization by the Executive Level Business Owner responsible for the operation of the MeF system and the explicit security.

Specific guidance is provided by various National Institute of Standards (NIST) special publications (the “800” series.) The process must include formal review and testing of the design and implementation of the system’s security controls. The IRS M&SSE organization and the business system owner were jointly responsible and actively involved in completing the IRS C&A Process for MeF.

The IRS operates continuous security status monitoring at the enterprise, network, and application levels. Computer security and incident response staff specialists actively manage these around the clock. Each year, IRS e-file systems are assessed by an independent

external security certification organization, and are also subject to audits by the Government Accountability Office (GAO) as well as the Treasury Inspector General for Tax Administration (TIGTA).

The IRS maintains a state of the art security posture, and interfaces with federal and commercial real-time security organizations (such as US-CERT, the SANS Internet Storm Center, and others) to keep a comprehensive view of their security state, and to update relevant software and systems as appropriate. The IRS also continues to incorporate new security technologies and procedures for detecting and preventing emerging threats and vulnerabilities such as those presented by SOAP and XML processing.

Privacy of Taxpayer Data

The IRS Office of Privacy is responsible for IRS policies and programs that protect taxpayer privacy after the tax return is filed. This office ensures that IRS programs and projects gather only the taxpayer data necessary to accomplish the Service's business objectives.

All IRS data processing systems and manual procedures used by IRS employees include features designed to enforce restrictions on access to account and tax return data to only those employees with a business need to know. IRS systems are designed to proactively prevent unauthorized employee access. All employees authorized to have access to tax return data automatically generate an audit log. IRS officials have a requirement to perform regular analysis on these employees. All IRS employees who may have inadvertently accessed case, account or tax return data not assigned to him or her as part of their work MUST report the incident and circumstances to his or her manager. The manager processes the report for possible further examination. TIGTA also conducts independent reviews to detect or discover any disclosure of tax data violations. Employees that violate the security and privacy rules may be disciplined according to the August 5, 1997 Taxpayer Browsing Protection Act, Public Law 105-35 (revised IRC 7213A) which provides for penalties including fines, imprisonment and dismissal of the employee.

All IRS systems that collect personally identifiable information are required to prepare Privacy Impact Assessments (PIA). Performing PIAs ensures that:

- The public is aware of the information the IRS collects
- Any impact these systems have on personal privacy is adequately addressed, and
- The IRS collects only enough personal information sufficient to administer its programs, and no more.

In addition, PIAs confirm that:

- The information is used for the purpose intended
- The information remains timely and accurate and that it is protected while in use, and
- Held only for as long as is needed.

PIAs are publicly available at: http://www.irs.gov/privacy/article/0,,id=122989,00.html
Third-party access to tax return data requires a Power of Attorney (POA) whether the return is filed on paper or electronically. A full registration, and application process is required for

third-party firms and individuals before they are approved by IRS to access IRS e-services. All other security controls remain in effect for third-party access.

IRS recognizes the importance of ensuring both the privacy and security of taxpayer information and delivering services that meet the highest standards of public trust. Corporations are encouraged to send specific security questions or concerns to largecorporate@irs.gov.